UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,696	11/23/2005	Gopala Krishna Srungaram	4544-051285	2673

28289 7590 02/10/2009

THE WEBB LAW FIRM, P.C.
700 KOPPERS BUILDING
436 SEVENTH AVENUE
PITTSBURGH, PA 15219

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,696	SRUNGARAM, GOPALA KRISHNA	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 4/26/2005.

DETAILED ACTION

Claims 12-21 have been examined.

Title

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The current title is not descriptive enough because "Elliptic Curve Encryption" provides no insight into what is different about this method from all other methods of Elliptic Curve Encryption.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 7/10/2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

Drawings

The drawings filed on 4/26/2005 are acceptable for examination proceedings.

Specification

The disclosure is objected to because of the following informalities: Due to the use of superscripts throughout the specification, the specification is not entirely legible. Please submit a replacement copy of the specification in order to ensure that there are no errors in the publication of this application in the future.

Appropriate correction is required.

Claim Objections

Claims 12-21 are objected to because of the following informalities:

Claim 12 Line 1 recites "the step of" but should read "the steps of".

Claim 12 Step ciii recites "multiplication of binary" but should read "multiplying the binary".

Claim 15 recites "size of M (in bits)". "in bits" should not be contained in parenthesis.

Appropriate correction is required.

The examiner notes that while the use of pseudo-code in the claims is not forbidden, its use renders the claims difficult to comprehend, and often times, as noted above and below, will introduce issues of clarity.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 12-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 12-21 recite a method containing mathematical equations and variables, such as 'p', 'I', 'M', 'T31', "result", "next" and many others. There is insufficient antecedent basis for this limitation in the claim. In other words, the variables are not defined in the claims. These can be fixed by defining the variables properly. For example, "setting a counter variable I to zero". This issue seems to have arisen because the claims are written mainly in pseudo-code. The

applicant is required to properly define all of the variables within the claims including the examples provided above.

Claims 12-21 recite numerous limitations for which there is insufficient antecedent basis in the claim. Some examples are listed below:

Claim 12 Step f: the input message MSG.

Claim 12 Step g: the ciphered text.

Claim 15 Step xxiv: function BSERIES (N, INCRE).

This list is not exhaustive. However, the applicant is required to correct all antecedent basis issues within the claims.

The terms "large", "small", "about", "big", and other similar terminology in the claims are relative terms which renders the claim indefinite. The terms are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The claim also recite numerous times "if true" and "if false". However, the claims do not indicate what needs to be true or false. As such, the ordinary person skilled in the art would not understand the scope of these limitations, thereby rendering the claims indefinite.

Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. In this case, steps a-e amount to simply manipulation of data. Steps f-g provide for encryption and decryption of data. However, claim 12 provides no connection between the abstract idea of steps a-e and the encryption/decryption of steps f-g. As such, the claim is rejected for being incomplete.

Claim Rejections - 35 USC § 101

Claim(s) 12-21 is/are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The elliptic curve encryption method is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 12-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over SEC (SEC 1: Elliptic Curve Cryptography), and further in view of Ye et al. (US Patent Application Publication 20040158597) hereinafter referred to as Ye.

Regarding claim 12, SEC disclosed a method of elliptic curve encryption comprising the step of: (a) selecting an elliptic curve E.sub.p (a,b) of the form y.sup.2=x.sup.3+ax+b mod (p) wherein a and b are non-negative integers less than p satisfying the formula 4 a.sup.3+27b.sup.2 mod (p) not equal to 0 (SEC Page 6 Section 2.2.1); (b) generating a large 160 bit random number by a method of concatenation of a number of smaller random numbers (SEC Page 22 Section 3.2.1); (c) generating a well hidden point G (x,y) on the elliptic curve E.sub.p (a,b) by scalar multiplication of a point B (x,y) on the elliptic curve with a large random integer (SEC Page 22 Section 3.2.1) (d) generating a private key n.sub.A (of about >=160 bit length) (SEC Page 22 Section 3.2.1); (e) generating of public key P.sub.A(x,y) given by the formula P.sub.A (x,y)=(n.sub.AG (x,y)) mod (p) (SEC Page 22 Section 3.2.1); (f) encrypting the input message MSG (SEC Page 42+ Section 5.1.3); (g) decrypting the ciphered text (SEC Page 43+ Section 5.1.4), but SEC did not specifically disclose the scalar multiplication comprising the steps: (i) converting the large random integer into a series of powers of 2.sup.31; (ii) converting each coefficient of 2.sup.31 obtained from above step into binary series; (iii) multiplication of binary series obtained from steps (i) and (ii) above with the point B (x,y) on the elliptic curve.

However, Ye teaches a method for scalar multiplication which comprises the steps: (i) converting the large random integer into a series of powers of 2.sup.31; (ii) converting each coefficient of 2.sup.31 obtained from above step into binary series; (iii) multiplication of binary series obtained from steps (i) and (ii) above with the point B (x,y) on the elliptic curve (Ye Paragraphs 0077-0099).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Ye in the system of SEC by performing the scalar

multiplication in the manner taught. This would have been obvious because the ordinary person skilled in the art would have been motivated to enhance performance of the system on 32-bit processors.

Regarding claim 13, SEC and Ye disclosed that the number p is about a 160 bit length prime number (SEC Page 16 Section 3.1.1).

Regarding claims 14-17, and 19-21, while SEC and Ye did not disclose these specific "instructions" for performing the elliptic curve encryption method, the particular manner in which the functional steps are "coded" is a matter of design choice, and as such would have been obvious to the ordinary person skilled in the art.

Regarding claim 18, SEC and Ye disclosed that the public key is also a point on the elliptic curve (SEC Page 22 Section 3.2.1 because multiplying an integer by a point on the elliptic curve produces another point on the elliptic curve).

Conclusion

Claims 12-21 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431